

OCTAVE[®]-S Implementation Guide, Version 1.0

Volume 8: Critical Asset Worksheets for People

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005



**Carnegie Mellon
Software Engineering Institute**

Pittsburgh, PA 15213-3890

OCTAVE[®]-S Implementation Guide, Version 1.0

Volume 8: Critical Asset Worksheets for People

CMU/SEI-2003-HB-003

Christopher Alberts
Audrey Dorofee
James Stevens
Carol Woody

January 2005

Networked Systems Survivability Program

Unlimited distribution subject to the copyright.

This report was prepared for the

SEI Joint Program Office
ESC/XPK
5 Eglin Street
Hanscom AFB, MA 01731-2100

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER



Christos Scodras
Chief of Programs, XPK

This work is sponsored by the U.S. Department of Defense. The Software Engineering Institute is a federally funded research and development center sponsored by the U.S. Department of Defense.

Copyright 2005 by Carnegie Mellon University.

® OCTAVE is registered in the U.S. Patent & Trademark Office by Carnegie Mellon University.

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

NO WARRANTY

THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

Use of any trademarks in this report is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be addressed to the SEI Licensing Agent.

This work was created in the performance of Federal Government Contract Number F19628-00-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

For information about purchasing paper copies of SEI reports, please visit the publications portion of our Web site (<http://www.sei.cmu.edu/publications/pubweb.html>).

Table of Contents

About This Documentv

Abstract.....vii

1 Introduction 1

2 Critical Asset Information Worksheet for People..... 5

3 Risk Profile Worksheet for People – Other Problems..... 9

4 Threat Translation Guide25

List of Tables

Table 1: Worksheets Provided in This Workbook	1
---	---

About This Document

This document is Volume 6 of the *OCTAVE-S Implementation Guide*, a 10-volume handbook supporting the OCTAVE-S methodology. This volume provides worksheets to document data related to critical assets that are categorized as people.

The volumes in this handbook are

- *Volume 1: Introduction to OCTAVE-S* – This volume provides a basic description of OCTAVE-S and advice on how to use the guide.
- *Volume 2: Preparation Guidelines* – This volume contains background and guidance for preparing to conduct an OCTAVE-S evaluation.
- *Volume 3: Method Guidelines* – This volume includes detailed guidance for each OCTAVE-S activity.
- *Volume 4: Organizational Information Workbook* – This volume provides worksheets for all organizational-level information gathered and analyzed during OCTAVE-S.
- *Volume 5: Critical Asset Workbook for Information* – This volume provides worksheets to document data related to critical assets that are categorized as information.
- *Volume 6: Critical Asset Workbook for Systems* – This volume provides worksheets to document data related to critical assets that are categorized as systems.
- *Volume 7: Critical Asset Workbook for Applications* – This volume provides worksheets to document data related to critical assets that are categorized as applications.
- ***Volume 8: Critical Asset Workbook for People*** – This volume provides worksheets to document data related to critical assets that are categorized as people.
- *Volume 9: Strategy and Plan Workbook* – This volume provides worksheets to record the current and desired protection strategy and the risk mitigation plans.
- *Volume 10: Example Scenario* – This volume includes a detailed scenario illustrating a completed set of worksheets.

Abstract

The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE[®]) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.

1 Introduction

This document contains the Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE[®])-S worksheets related to critical assets that are people. The activities related to these worksheets are focused on analyzing a critical asset.

Table 1 provides a brief introduction to the contents of this workbook, using activity step numbers as a key. For more details about how to complete each step, refer to the *OCTAVE[®]-S Method Guidelines*, which can be found in Volume 3 of the *OCTAVE[®]-S Implementation Guide*.

Table 1: Worksheets Provided in This Workbook

Step	Description	Worksheet	Activity	Pages
Step 6	Start a <i>Critical Asset Information worksheet</i> for each critical asset. Record the name of the critical asset on its <i>Critical Asset Information worksheet</i> .	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 7	Record your rationale for selecting each critical asset on that asset's <i>Critical Asset Information worksheet</i> .	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 8	Record a description for each critical asset on that asset's <i>Critical Asset Selection worksheet</i> . Consider who uses each critical asset as well as who is responsible for it.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 9	Record assets that are related to each critical asset on that asset's <i>Critical Asset Information worksheet</i> . Refer to the <i>Asset Identification worksheet</i> to determine which assets are related to each critical asset.	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8

SM Operationally Critical Threat, Asset, and Vulnerability Evaluation is a service mark of Carnegie Mellon University.

[®] OCTAVE is registered in the United States Patent and Trademark Office by Carnegie Mellon University.

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 10	Record the security requirements for each critical asset on that asset's <i>Critical Asset Information worksheet</i> .	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 11	For each critical asset, record the most important security requirement on that asset's <i>Critical Asset Information worksheet</i> .	Critical Asset Information	Phase 1 Process S2 S2.1 Select Critical Assets	5-8
Step 12	Complete all appropriate threat trees for each critical asset. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset. If you have difficulty interpreting a threat on any threat tree, review the description and examples of that threat in the <i>Threat Translation Guide</i> .	Risk Profile Threat Translation Guide	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-24
Step 15	Record how often each threat has occurred in the past. Also record how accurate you believe your data are.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-24
Step 16	Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.	Risk Profile	Phase 1 Process S2 S2.1 Identify Threats to Critical Assets	9-24
Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) for each active threat to each critical asset.	Risk Profile Impact Evaluation Criteria	Phase 3 Process S4 S4.1 Evaluate Impacts of Threats	9-24
Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) for each active threat to each critical asset. Document your confidence level in your probability estimate.	Risk Profile Probability Evaluation Criteria	Phase 3 Process S4 S4.3 Evaluate Probabilities of Threats	9-24

Table 1: Worksheets Provided in This Workbook (cont.)

Step	Description	Worksheet	Activity	Pages
Step 26	Transfer the stoplight status for each security practice area from the <i>Security Practices worksheet</i> to the “Security Practice Areas” section (Step 26) of each critical asset’s <i>Risk Profile worksheet</i> .	Risk Profile Security Practices	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-24
Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.	Risk Profile	Phase 3 Process S5 S5.2 Select Mitigation Approaches	9-24

2 Critical Asset Information Worksheet for People

Phase 1
Process S2
Activity S2.1

Step 6	Start a <i>Critical Asset Information worksheet</i> for each critical asset. Record the name of the critical asset on its <i>Critical Asset Information worksheet</i> .
---------------	---

Step 7	Record your rationale for selecting each critical asset on that asset's <i>Critical Asset Information worksheet</i> .
---------------	---

Step 8	Record a description for each critical asset on that asset's <i>Critical Asset Selection worksheet</i> . Consider who uses each critical asset as well as who is responsible for it.
---------------	--

Step 9	Record assets that are related to each critical asset on that asset's <i>Critical Asset Information worksheet</i> . Refer to the <i>Asset Identification worksheet</i> to determine which assets are related to each critical asset.
---------------	--

Phase 1
Process S2
Activity S2.2

Step 10	Record the security requirements for each critical asset on that asset's <i>Critical Asset Information worksheet</i> .
----------------	--

Step 11	For each critical asset, record the most important security requirement on that asset's <i>Critical Asset Information worksheet</i> .
----------------	---

Step 6	Step 7
Critical Asset	Rationale for Selection
<i>What is the critical person(s)?</i>	<i>Why is this person(s) critical to the organization?</i>

Step 9
Related Assets
<i>Which assets are related to this person(s)?</i>
<div>Systems:</div> <div>Information:</div> <div>Applications:</div> <div>Other:</div>

Step 8

Description

What special skills or knowledge are provided by this person(s)?

--

Step 10

Security Requirements

What are the security requirements for this person(s)?

(Hint: Focus on what the security requirements should be, not what they currently are.)

☐ Availability The set of skills provided by_____ must be available when needed.

☐ Other _____

Step 11

Most Important Security Requirement

Which security requirement is most important for this person(s)?

☐ Availability

☐ Other

3 Risk Profile Worksheet for People – Other Problems

Phase 1
Process S2
Activity S2.3

Step 12	<p>Complete the threat tree for <i>other problems</i>. Mark each branch of each tree for which there is a non-negligible possibility of a threat to the asset.</p> <p>If you have difficulty interpreting a threat on the threat tree, review the description and examples of that threat in the <i>Threat Translation Guide</i> (see pp. 26-30 of this workbook).</p>
Step 15	<p>Record how often each threat has occurred in the past. Also record how accurate you believe your data are.</p>
Step 16	<p>Record areas of concern for each source of threat where appropriate. An area of concern is a scenario defining how specific threats could affect the critical asset.</p>

continued

Phase 3
Process S4
Activity S4.1

Step 22	Using the impact evaluation criteria as a guide, assign an impact value (high, medium, or low) to each active threat.
----------------	---

Phase 3
Process S4
Activity S4.3

Step 24	Using the probability evaluation criteria as a guide, assign a probability value (high, medium, or low) to each active threat. Document your confidence level in your probability estimate.
----------------	---

Phase 3
Process S5
Activity S5.2

Step 26	Transfer the stoplight status for each security practice area from the <i>Security Practices worksheet</i> to the “Security Practice Areas” section (Step 26) of the following worksheet.
----------------	---

Step 27	Select a mitigation approach (mitigate, defer, accept) for each active risk. For each risk that you decided to mitigate, circle one or more security practice areas for which you intend to implement mitigation activities.
----------------	---

Other Problems			Basic Risk Profile						
Step 12			Step 22						
Threat			Impact Values						
<p>For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.</p> <p>For which of the remaining branches is there a negligible possibility or no possibility of a threat to the asset? Do not mark these branches.</p>			<p>What is the potential impact on the organization in each applicable area?</p>						
Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other	
	key people taking a temporary leave of absence (e.g., due to illness, disability)	disclosure							
		modification							
		loss, destruction							
		interruption							
	key people leaving the organization permanently (e.g., retirement, other opportunities)	disclosure							
		modification							
		loss, destruction							
		interruption							
	threats affecting a third-party or service provider	disclosure							
		modification							
		loss, destruction							
		interruption							
		disclosure							
		modification							
		loss, destruction							
		interruption							

Basic Risk Profile

Other Problems

Step 24

Step 26

Step 27

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Security Practice Areas

What is the stoplight status for each security practice area?

Approach

What is your approach for addressing each risk?

Value

Confidence

Strategic

Operational

Very

Somewhat

Not At All

1. Sec Training

2. Sec Strategy

3. Sec Mgmt

4. Sec Policy & Reg

5. Coll Sec Mgmt

6. Cont Planning

7. Phys Acc Cntrl

8. Monitor Phys Sec

9. Sys & Net Mgmt

10. Monitor IT Sec

11. Authen & Auth

12. Vul Mgmt

13. Encryption

14. Sec Arch & Des

15. Incident Mgmt

Accept

Defer

Mitigate

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

☐

-----|-----|-----

--	--	--	--	--	--	--

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------	--------------------------

Other Problems		Threat Context	
		Step 15	
		History	
		<i>How often has this threat occurred in the past?</i>	<i>How accurate are the data?</i>
			Very Somewhat Not At All
	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
key people taking a temporary leave of absence (e.g., due to illness, disability)	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
key people leaving the organization permanently (e.g., retirement, other opportunities)	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
threats affecting a third-party or service provider	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

[illegible]

Step 16

Other Problems

Areas of Concern

People Taking a Temporary Leave of Absence

Give examples of how *key people taking a temporary leave of absence* could affect the ability of this person or group of people to provide critical services, skills, and knowledge.

People Leaving the Organization Permanently

Give examples of how *key people leaving the organization permanently* could affect the ability of this person or group of people to provide critical services, skills, and knowledge.

Threats Affecting a Third-Party

Give examples of how *threats affecting a third party or service provider* could affect the ability of that third-party or service provider to provide critical services, skills, and knowledge.

Give examples of how

_____ could affect the ability of this person or group of people to provide critical services, skills, and knowledge.

Areas of Concern

	People Taking a Temporary Leave of Absence
	People Leaving the Organization Permanently
	Threats Affecting a Third-Party

Other Problems (cont.)			Basic Risk Profile						
Step 12			Step 22						
Threat			Impact Values						
<p>For which branches is there a non-negligible possibility of a threat to the asset? Mark these branches on the tree.</p> <p>For which of the remaining branches is there a negligible possibility of a threat to the asset? Do not mark these branches.</p>			<p>What is the potential impact on the organization in each applicable area?</p>						
Asset	Actor	Outcome	Reputation	Financial	Productivity	Fines	Safety	Other	
<div style="border: 1px solid black; width: 80px; height: 120px; margin: 10px auto;"></div>		disclosure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		modification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		loss, destruction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		interruption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		disclosure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		modification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		loss, destruction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		interruption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		disclosure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		modification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		loss, destruction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		interruption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		disclosure	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		modification	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		loss, destruction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		interruption	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Basic Risk Profile

Other Problems (cont.)

Step 24

Step 26

Step 27

Probability

How likely is the threat to occur in the future? How confident are you in your estimate?

Value

Confidence

Very

Somewhat

Not At All

Strategic

Operational

Security Practice Areas

What is the stoplight status for each security practice area?

Approach

What is your approach for addressing each risk?

1. Sec Training

2. Sec Strategy

3. Sec Mgmt

4. Sec Policy & Reg

5. Coll Sec Mgmt

6. Cont Planning

7. Phys Acc Cntrl

8. Monitor Phys Sec

9. Sys & Net Mgmt

10. Monitor IT Sec

11. Authen & Auth

12. Vul Mgmt

13. Encryption

14. Sec Arch & Des

15. Incident Mgmt

Accept

Defer

Mitigate

☐☐☐

Other Problems (cont.)		Threat Context													
		Step 15													
		<table border="1"> <thead> <tr> <th colspan="2">History</th> </tr> </thead> <tbody> <tr> <td><i>How often has this threat occurred in the past?</i></td> <td><i>How accurate are the data?</i></td> </tr> <tr> <td></td> <td> <table border="1"> <thead> <tr> <th>Very</th> <th>Somewhat</th> <th>Not At All</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table> </td> </tr> </tbody> </table>		History		<i>How often has this threat occurred in the past?</i>	<i>How accurate are the data?</i>		<table border="1"> <thead> <tr> <th>Very</th> <th>Somewhat</th> <th>Not At All</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Very	Somewhat	Not At All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
History															
<i>How often has this threat occurred in the past?</i>	<i>How accurate are the data?</i>														
	<table border="1"> <thead> <tr> <th>Very</th> <th>Somewhat</th> <th>Not At All</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </tbody> </table>	Very	Somewhat	Not At All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>								
Very	Somewhat	Not At All													
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>													
	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	disclosure	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	modification	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	loss, destruction	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												
	interruption	_____ times in _____ years	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>												

[illegible]

Step 16**Other Problems (cont.)****Areas of Concern**

<p>Give examples of how</p> <hr/> <p>could affect the ability of this person or group of people to provide critical services, skills, and knowledge.</p>	
<p>Give examples of how</p> <hr/> <p>could affect the ability of this person or group of people to provide critical services, skills, and knowledge.</p>	
<p>Give examples of how</p> <hr/> <p>could affect the ability of this person or group of people to provide critical services, skills, and knowledge.</p>	
<p>Give examples of how</p> <hr/> <p>could affect the ability of this person or group of people to provide critical services, skills, and knowledge.</p>	

Areas of Concern

[illegible]

4 Threat Translation Guide

Phase 1
Process S2
Activity S2.3

Threat Translation Guide	The <i>Threat Translation Guide</i> describes each branch of an asset-based threat tree. If you have difficulty understanding the types of threats represented by a branch, you can use this guide to decipher the meaning of that branch.	
	You will find asset-based threat trees for the following sources of threat:	
	Source of Threat	Page
	Other problems	26-30

Other Problems		
Asset	Actor	Outcome
		disclosure
		modification
	key people taking a temporary leave of absence (e.g., due to illness, disability)	loss, destruction
		interruption
		disclosure
	key people leaving the organization permanently (e.g., retirement, other opportunities)	modification
		loss, destruction
		interruption

* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
---	---
---	---
---	---
<p>A staff member(s) with unique knowledge or a unique skill takes a temporary leave of absence from an organization. The organization does not have any other staff members with comparable skills, resulting in an interruption of access to the unique knowledge or skill.</p>	<p>A key member of the IT group in a small organization takes a leave of absence to care for an ill family member. This member of the IT staff is responsible for maintaining a legacy order entry system. No other staff members know how to maintain the system. The organization has a temporary interruption of access to a vital skill that is important to its business operations.</p>
---	---
---	---
---	---
---	---
<p>A staff member(s) with unique knowledge or a unique skill leaves an organization permanently. The organization does not have any other staff members with comparable skills, resulting in an interruption of access to the unique knowledge or skill until a replacement is hired.</p>	<p>A clerk is responsible for entering data into a database system. The clerk, who is currently the only one at the company who understands how to use the system, unexpectedly leaves for a better position at another company. The organization no longer has access to a skill that is important to its business operations until a replacement is hired and trained.</p>

Other Problems		
Asset	Actor	Outcome
<div></div>		disclosure
		modification
		loss, destruction
		interruption
		disclosure
		modification
		loss, destruction
		interruption
	threats affecting a third-party or service provider	

* Blank lines indicate unusual or extremely rare possibilities.

Description	Example*
---	---
---	---
---	---
An organization depends on a third party for a particular service. Any threats to the third party that prevents them from fulfilling their obligations results in an interruption of service to the organization.	A service provider maintains the computing infrastructure for a manufacturing company. A shop floor scheduling system is physically located at the service provider's site. A disgruntled staff member employed by the service provider plants a software "time bomb" that takes down the service provider's networks for several days. The manufacturing site's access to the shop floor scheduling system is interrupted until the service provider can get its infrastructure running again.

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.				
1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE January 2005		3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE OCTAVE-S Implementation Guide, Version 1.0, Volume 8			5. FUNDING NUMBERS F19628-00-C-0003	
6. AUTHOR(S) Christopher Alberts, Audrey Dorofee, James Stevens, Carol Woody				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213			8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2003-HB-003	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS			12B DISTRIBUTION CODE	
13. ABSTRACT (MAXIMUM 200 WORDS) The Operationally Critical Threat, Asset, and Vulnerability Evaluation SM (OCTAVE [®]) approach defines a risk-based strategic assessment and planning technique for security. OCTAVE is a self-directed approach, meaning that people from an organization assume responsibility for setting the organization's security strategy. OCTAVE-S is a variation of the approach tailored to the limited means and unique constraints typically found in small organizations (less than 100 people). OCTAVE-S is led by a small, interdisciplinary team (three to five people) of an organization's personnel who gather and analyze information, producing a protection strategy and mitigation plans based on the organization's unique operational security risks. To conduct OCTAVE-S effectively, the team must have broad knowledge of the organization's business and security processes, so it will be able to conduct all activities by itself.				
14. SUBJECT TERMS information security, risk management, OCTAVE			15. NUMBER OF PAGES 30	
16. PRICE CODE				
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	